UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,668	12/19/2000	Akira Nonaka	450100-02904	7062

20999 7590 06/01/2004

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	5

DATE MAILED: 06/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/741,668	NONAKA ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) *23-56* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-22, drawn to a tamper resistant data rights processing apparatus, classified in class 713, subclass 194.

   II. Claims 23-32 and 42-49, drawn to systems and a method for managing usage of distributed data files, classified in class 707, subclass 10.

   III. Claims 33-41 and 50-56, drawn to systems and methods performing mutual authentication, classified in class 713, subclass 169.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I and II are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the combination (invention II) does not specify an arithmetic processing circuit, buses, or an interface circuit as in the subcombination (invention I). The subcombination has separate utility such as performing data processing according to a different method or in a different system.

3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

4. Inventions I and III are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the combination (invention III) broadly recites a "tamper-resistant data processing apparatus" but does not specify the particulars of the subcombination (invention I). The subcombination has separate utility such as performing data processing according to a different method or in a different system.

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

6. Inventions II and III are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the combination (invention III)

does not specify the determining means, log data generating means, or decrypting means of the subcombination (invention II). The subcombination has separate utility such as performing usage rights management for distributed data.

7. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

8. During a telephone conversation with William Frommer on 18 May 2004 a provisional election was made with traverse to prosecute the invention of Group I, claims 1-22. Affirmation of this election must be made by applicant in replying to this Office action. Claims 23-56 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

9. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Drawings

10. Figure 106 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

11. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "1130" has been used to designate both the I^2C bus in Figure 69 and the tamper resistant software in Figure 72. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

12. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 1123 (see page 164 of the specification). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

13. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 1407 (see Figure 69). A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are

required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

14. The disclosure is objected to because of the following informalities:

The specification and claims do not include line numbers. See MPEP § 608.01.

On page 163, lines 17-19, reference is made to "mask ROM 1104" and "non-volatile memory 1105" in Figure 69. However, reference number 1104 is not included in Figure 69, nor is there a "mask ROM" included in the figure. Further, it is unclear if reference number 1105 indicates "non-volatile memory" as reference number 1105 appears to indicate "code" and "data" in the "FLASH-ROM" which is not numbered.

Appropriate correction is required.

15. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 101

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. Claims 17-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 17 is directed to both an apparatus and method steps of using that apparatus. The claim is therefore not directed to either a process or a machine, but instead overlaps the two statutory classes of invention. This renders the claims non-statutory. See MPEP § 2173.05(p)II.

18. To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 above are further rejected as set forth below in anticipation of applicant amending these claims to place them with in the statutory classes of invention.

Claim Rejections - 35 USC § 112

19. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

20. Claims 5-7, 10, 14, and 17-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 recites the limitation "the corresponding public key data" in lines 9-10. There is insufficient antecedent basis for this limitation in the claim. Further, the claim recites the limitation "them" in line 12. It is unclear what this limitation refers to. For purposes of applying prior art, the limitation is assumed to refer to "the content data, the content key data, and the usage control policy data" of lines 10-11.

Claim 6 is rejected due to its dependence on rejected Claim 5.

Claim 7 recites the limitation "said second data processing apparatus" in lines 6 and 8-9. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation "a host arithmetic processing apparatus for centrally controlling a system on which said data processing apparatus is loaded" in lines 3-5. The phrase "on which said data processing apparatus is loaded" is unclear as a limitation of "a system", as the claims are directed solely to a data processing apparatus and not to a system. This limitation renders the claim indefinite.

Claim 14 recites the limitation "the purchase mode" in lines 2-3 and the limitation "the usage control status data" in line 5. There is insufficient antecedent basis for these limitations in the claim.

Claim 17 is directed to both an apparatus and method steps for using that apparatus, which is ambiguous, as it is unclear whether the apparatus or the method is being claimed. This renders the claim indefinite. See MPEP § 2173.05(p)II.

Claims 18-22 are rejected due to their dependence on rejected Claim 17.

Claim Rejections - 35 USC § 102

21. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

22. Claims 1-8, 10, and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al, US Patent 5768382.

In reference to Claim 1, Schneier discloses an apparatus within a tamper-resistant circuit module (column 8, lines 17-27; column 11, lines 31-37) including a first bus (see Figures 4C-4H), an arithmetic processing circuit (Figure 4C, CPU 302), a storage circuit (Figure 4C, ROM 304), a second bus (see Figures 4C-4H), an interface circuit (see Figure 4C), an encryption processing circuit (Figure 4B-4C, encryption/decryption module 28; also column 11, lines 41-46), and an external bus interface circuit (Figure 4C, I/O 312).

In reference to Claim 2, Schneier further discloses a second interface circuit and that the first bus includes a third bus and a fourth bus (see Figures 4C-4H).

In reference to Claim 3, Schneier further discloses a third interface circuit communicating with a recording medium (Figure 4H, interface circuitry 406), a fifth bus, and a fourth interface circuit (see Figures 4C-4H).

In reference to Claim 4, Schneier further discloses a public key encryption circuit (column 10, lines 27-56) and a common key encryption circuit (column 9, line 62-column 10, line 11).

In reference to Claim 5, Schneier further discloses that the storage circuit stores private and public key data (column 11, lines 44-48), the public key encryption circuit verifies the integrity of signature data and creates signature data (column 10, lines 41-56), and the common key encryption circuit encrypts and decrypts content data and key data using a session key (column 9, line 65-column 10, line 6).

In reference to Claim 6, Schneier further discloses a hash value generating circuit used by the public key encryption circuit in verifying and creating signatures (column 17, lines 46-50).

In reference to Claim 7, Schneier further discloses a random number generating circuit (column 10, lines 57-67).

In reference to Claim 8, Schneier further discloses an external storage circuit (column 7, lines 57-60).

In reference to Claim 10, Schneier further discloses that the external bus is connected to a host processor (see Figure 4C, where the I/O 312 is connected to external CPU 27).

In reference to Claim 16, Schneier further discloses that the storage circuit writes and erases data in units of blocks and also discloses a write lock control circuit for controlling writing and erasing blocks of data (column 18, lines 39-43).

In reference to Claim 17, Schneier discloses an apparatus within a tamper-resistant circuit module (column 8, lines 17-27; column 11, lines 31-37) including a first bus (see Figures 4C-4H), an arithmetic processing circuit (Figure 4C, CPU 302), a storage circuit (Figure 4C, ROM 304), a second bus (see Figures 4C-4H), an interface circuit (see Figure 4C), an encryption processing circuit (Figure 4B-4C, encryption/decryption module 28; also column 11, lines 41-46), and an external bus interface circuit (Figure 4C, I/O 312). Schneier further discloses receiving an interrupt

from an external circuit, performing processing, and reporting a result of the processing (column 11, lines 55-67).

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. Claims 9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier.

Schneier discloses everything as applied to Claim 8 above. Schneier further discloses that programs are executed from memory in a conventional manner (column 7, lines 60-61). However, Schneier does not explicitly disclose a storage-circuit control circuit or a storage management circuit.

Official notice is taken that it is well known in the computer arts to include a memory controller or memory management circuit, such as a DMA or MMU, in order to allow for the optimization of the use of memory.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including a memory controller or manager, in order to optimize the use of memory, as is well known in the computer arts.

25. Claims 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Christiano, US Patent 5671412.

In reference to Claim 12, Schneier discloses everything as applied to Claim 1 above. However, Schneier does not explicitly disclose determining a mode based on a handling policy and creating log data.

Christiano discloses determining a usage or purchase mode based on a usage license policy (column 6, line 60-column 7, line 30) and logging data (column 18, lines 53-61).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including the usage policies and licensing as disclosed by Christiano, in order to provide a variety of options and flexibility in controlling usage of licensed data (see Christiano, column 3, lines 12-19).

In reference to Claim 13, Christiano further discloses creating usage control status data (column 10, lines 53-57) and controlling use of content data (column 10, line 64- column 11, line 3).

In reference to Claims 14 and 15, Schneier discloses everything as applied to Claim 4 above. In reference to Claim 15, Schneier further discloses a real time clock (column 11, line 46). However, Schneier does not explicitly disclose encrypting content

key data and usage control status data, nor does Schneier disclose storing license key data.

Christiano discloses encrypting key data and control data (column 14, lines 23-28) and storing license key data (column 14, lines 19-21).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including the usage policies and licensing as disclosed by Christiano, in order to provide a variety of options and flexibility in controlling usage of licensed data (see Christiano, column 3, lines 12-19).

26. Claims 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Castor et al, US Patent 5590288.

In reference to Claims 18 and 19, Schneier discloses everything as applied to Claim 17 above. However, Schneier does not explicitly disclose reporting the result of processing by outputting an interrupt. Further, Schneier does not explicitly disclose that the external bus interface includes a common memory and that the external circuit obtains a result by polling.

Castor discloses a system which allows a computer to request another computer to execute a procedure (column 3, lines 38-42) including outputting an interrupt (column 12, lines 29-33). Castor further discloses a common memory (the buffer of column 12, lines 33-35) and polling an interface circuit to obtain a result (column 12, lines 35-47).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Schneier by including the interrupt, buffer, and polling of Castor, in order to increase reliability, lower cost, and allow easier upgrades in a distributed computing system (Castor, column 4, lines 11-21).

In reference to Claim 20, Castor further discloses first status registers including flags (column 12, lines 29-35).

In reference to Claim 21, Castor further discloses storing and executing an interrupt program (column 5, lines 49-51).

In reference to Claim 22, Castor further discloses storing and executing a plurality of interrupt programs and subroutines (column 5, lines 49-55).

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Chorley et al, US Patent 4634807, discloses a system for decrypting including a processor and memory within a tamper-resistant housing.

b. Smith, US Patent 4731842, discloses a security module including cryptographic processors in a tamper-proof housing.

c. Hampson, US Patent 4847902, discloses a system including a processor, memory, and decryptor within a tamper-proof enclosure.

d. Bernobich et al, US Patent 5812664, discloses a system including a processor, encryptor, and memory within a secure enclosure.

e. Atalla, US Patent 5960086, discloses a secure system including a processor and security data files enclosed in a tamper-proof box.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137